ABSTRACT

In a method for generating an identification value for identifying an electronic message by application of a first hash function with fixed compression that compresses n blocks of data into a number of blocks, which is smaller than n, the hash function is repetitively applied in a tree-structure compression of the message. The message is compressed in a plurality of tree-structure levels, each level receiving m_i input blocks for compression. One or more residual data blocks are treated by an auxiliary hash function or passed without compression from the current level to another subsequent level, in case n does not divide the number of input blocks at a particular level. A further method is provided, in which a number representation of a block of data is added to a number resulting from a hash operation. The methods of the invention may define MAC (Message Authentication Code) functions.